

CLAIMS

What is claimed is:

1. A data service system, comprising:
 - a plurality of web servers, each servicing any request received by the data service system;
 - a plurality of application servers, each processing any request directed from any one of the web servers;
 - a session state information managing system called by each of the application servers to allow different application servers to process requests belonging to a single session without requiring the requests to carry their entire session state information, wherein processing of each of the requests requires the session state information of that request.
2. The data service system of claim 1, wherein the session state information managing system further comprises
 - a session state information manager called by any one of the application servers when that application server processes a request of a session to (1) provide the session state information of the request to the application server and (2) generate a state reference for a new session state information for that request after the application server has processed the request and generated the new session state information for that request;
 - a store that stores all session state information received by the session state information manager.
3. The data service system of claim 2, wherein the state reference

generated is unique to the corresponding session state information and is a short and fixed length character string.

4. The data service system of claim 3, wherein the session state information manager generates the state reference by

- mapping the session state information to a sequence of bytes using a marshaling algorithm;
- mapping the sequence of bytes to a digest using a cryptographic hash algorithm;
- mapping the digest to the character string using an encoding algorithm, thus forming the state reference.

5. The data service system of claim 4, wherein the marshaling algorithm further comprises the property that can un-marshall the sequence of bytes into a replica of the session state information data structure without any loss of data.

6. The data service system of claim 4, wherein the digest mapped by the cryptographic hash algorithm is a fixed length, short sequence of bytes that is unique to the sequence of bytes.

7. The data service system of claim 4, wherein the encoding algorithm maps each byte in the digest to its hexadecimal representation, and creates the resulting character string.

8. A session state information managing system in a data service

system having a plurality of duplicate application servers, each for processing requests, comprising:

a session state information manager called by any one of the application servers when that application server processes a request of a session to (1) provide the session state information of the request to the application server and (2) generate a state reference for a new session state information for that request after the application server has processed the request and generated the new session state information for that request;

a store that stores all session state information received by the session state information manager.

9. The session state information managing system of claim 8, wherein the state reference generated is unique to the corresponding session state information and is a short and fixed length character string.

10. The session state information managing system of claim 9, wherein the session state information manager generates the state reference by mapping the session state information to a sequence of bytes using a marshaling algorithm;

mapping the sequence of bytes to a digest using a cryptographic hash algorithm;

mapping the digest to the character string using an encoding algorithm, thus forming the state reference.

11. The session state information managing system of claim 10, wherein the marshaling algorithm further comprises the property that can un-

marshal the sequence of bytes into a replica of the session state information data structure without any loss of data.

12. The session state information managing system of claim 10, wherein the digest mapped by the cryptographic hash algorithm is a fixed length, short sequence of bytes that is unique to the sequence of bytes.

13. The session state information managing system of claim 10, wherein the encoding algorithm maps each byte in the digest to its hexadecimal representation, and creates the resulting character string.

14. A method of allowing different application servers in a data service system to process requests belonging to a single session, comprising

(A) determining if a request starts a session;

if the request initiates the session, then

(B1) processing the request in one of the application servers and sending session state information of the request to a session state information manager;

(B2) receiving a state reference unique to the session state information from the session state information manager and attaching the state reference to the response to the request;

if the request does not start the session, then

(C1) retrieving the session state information associated with the request from the session state information manager using a state reference contained in the request;

(C2) processing the request with the retrieved session state

information in one of the application servers and generating a new session state information;

(C3) sending the new session state information of the request to the session state information manager to receive a new state reference unique to the new session state information and attaching the state reference to the response to the request.

15. The method of claim 14, wherein the step (C1) further comprises the steps of

verifying the session state information retrieved;

if the session state information is not verifiable, then performing the step (B1);

if the session state information is verified, then performing the step (C2).

16. The method of claim 14, wherein the session state information manager generates the state reference by

mapping the session state information to a sequence of bytes using a marshaling algorithm;

mapping the sequence of bytes to a digest using a cryptographic hash algorithm;

mapping the digest to the character string using an encoding algorithm, thus forming the state reference.